Before the
Federal Communication Commission
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 02-6
Schools and Libraries Universal Service	)	GN Docket No. 09-51
Support Mechanism	)	WC Docket No. 13-184
	)	

COMMENTS OF FUNDS FOR LEARNING, LLC *on the* DRAFT ELIGIBLE SERVICES LIST FOR SCHOOLS AND LIBRARIES UNIVERSAL SERVICE PROGRAM FOR FUNDING YEAR 2016

Funds for Learning ("FFL") is an E-rate-compliance consulting firm that services clients nationwide. Since 1997, we have been assisting our growing number of clients with the E-rate process. FFL has designed and continued to develop its online E-rate management and compliance service tool, E-rate Manager® ("ERM"). The resources that ERM offers to clients are invaluable. Clients are able to file E-rate applications, monitor the status of their applications and funding, archive documentation, and prepare for E-rate compliance.

FFL's clients come to us with their own set of assets and experiences. This provides us with a unique perspective into the world of E-rate. As we have grown and developed with the changing regulations, we are able to perceive how our clients have adapted as well. FFL has the opportunity to help navigate this process with our clients. We are able to see how rules are being misinterpreted, including the eligible services list.

In its *ESL Public Notice* for FY2015, the Commission states that:

> [t]he proposed ESL eliminates the list of ineligible services that had been posted at the end of each category of service. Although there are instances where these lists could prove helpful, providing applicants long lists of examples to review and understand has not been a fast, simple, or efficient aspect of the application process. Also, rather than examining long lists of ineligible services, it will be more efficient for applicants to assume that any service or component not listed in the ESL is ineligible for E-rate support.

While Funds For Learning continues to support this approach, we note that it can only be "more efficient" when the list of eligible services is tightly defined and unambiguous. In most cases, this proves to be true. For example, a device like a wireless access point has a reasonably consistent marketplace definition. Certainly, minor feature differences exist between manufacturers, but in terms of overall (or primary) functionality an access point is widely considered to be a single purpose device.

Other areas of the Eligible Services List, however, are not so clear. As a result, we observe a significant amount of confusion among equipment manufacturers, service providers, applicants, and consultants when it comes to the eligibility of eligible firewalls, software, and network management and monitoring functions. In these cases, we believe that much of the confusion stems from inconsistencies in the *marketplace* definition and understanding of the functionality provided by these services as compared to the Commission's (and/or USAC's) apparent definition. As a result, stakeholders acting in good faith may claim that a product or service is eligible based on their own interpretation of functionality (driven primarily by current marketplace standards) only to be surprised by funding denial or request for cost-allocation later in the E-rate's Program Integrity Assurance (or worse yet, invoicing) process. This creates a perceived inconsistency in funding decisions, which is frustrating at best (and perceived as anti-competitive at worst.)

While the FY2015 ESL *Order* "direct[s] USAC to include an ESL Glossary on its webpage," a glossary was not available during the FY2015 Form 471 filing window, and has not been added to USAC's website as of the date of this comment. As such, we urge the Commission to consider refining the definitions of firewall functionality, software components, and network monitoring/management functions in order to mitigate confusion among stakeholders during the planning stages of the E-rate process, as well as promote efficiency in the administrator's eligibility review and auditing process.

THE MARKETPLACE DEFINITION OF A "FIREWALL" IS INCONSISTENT WITH CURRENT ELIGIBLE SERVICES DEFINITIONS AND SHOULD BE CLARIFIED

Gartner estimates that in 2014, organizations spent over $70 billion worldwide on information security technologies.[1] Major data breaches at large companies like Target and The Home Depot illustrate a concept that is easy to grasp: protecting the sensitive data that traverses networks is paramount, and it's becoming more critical – and more difficult – year over year.

Our nation's schools are certainly not immune to this phenomenon. As sensitive student data like grades, transcripts, and test results increasingly become a part of the traffic flowing across both local and wide area networks, schools are being forced to implement proactive network security solutions in order to ensure student safety.

The simple fact is this: in 2015, schools **must** deploy network security solutions. Like most commercial organizations, they must offer protection from attacks that originate from outside the network (e.g. the public Internet.) Further, as more and more schools deploy one-to-one computing or BYOD (bring-your-own-device) initiatives, it is increasingly clear that offering protection from rogue devices connected to the local area network becomes a practical requirement as well. Without adequate protection, networks crash – and unreliable networks, in our opinion, certainly fall short of the program's overall goal.

It is clear that the Commission understands the importance of network security, as evidenced by its inclusion of firewalls as eligible components since Funding Year 2004. But in 2015, the marketplace definition of a "firewall" has changed. Certainly, circa-2005 firewall technologies still exist and are

[1] http://www.gartner.com/newsroom/id/2828722

widely deployed, but as networks have increased in complexity, so have the technical functions and features included in a “firewall” device. Commonly deployed security functions now include:

- Stateful packet inspection and “port blocking”
- Deep packet inspection and intrusion prevention
- Application layer firewalling/security
- Content security (including content filtering, spam control, and virus/malware protection)
- Network Access Control (NAC), user authentication, and access control gateway solutions

In practice, a device marketed as a “next generation firewall” – as well as the device that network administrators would colloquially refer to as “the firewall” – may well perform some or all of these features. “Basic” port-blocker firewall functionality is certainly included in these solutions, but the industry standard is rapidly evolving, as is the new definition of what a “basic” firewall entails.

In examining USAC’s funding decision results and explanations for Priority Two funding requests from Funding Year 2012 and prior (as well as early funding decisions for FY2015), it appears that the Commission’s (and/or USAC’s) intent is to fund only the firewall functionality first added to the Eligible Services List in Funding Year 2004, resulting in the denial (or cost-allocation) of many next-generation firewall/security products.

We make no comment on which next-generation network security functions/features should be eligible in Funding Year 2016. However, it is very clear to us that a **significant** amount of confusion is created among E-rate stakeholders when the Eligible Services List contains “firewalls” as eligible components, because a majority of stakeholders now view a “firewall” as a security device that combines one or more methods of threat protection. We therefore suggest that the Commission consider clarifying its intent when it comes to network security through modifications to the Eligible Services List, the use of a glossary of terms, or an *Order* which provides more detail. We suggest that the definition/clarification clearly address the areas of technical functionality provided above, as well as whether eligible firewalls include threat protection at the network edge only (e.g. protection from the public Internet), or if an eligible firewall may also include authentication or network access control services (user identification and protection from internal/third-party devices accessing an applicant’s local area network.)

THE ELIGIBLE SERVICES LIST’S TREATMENT OF NETWORK MONITORING AND MANAGEMENT FUNCTIONALITY IS INCONSISTENT, AND SHOULD BE CLARIFIED

As a result of program policy changes in the Commission’s *Seventh Report and Order*, the FY2015 Eligible Services List was updated to include the Managed Internal Broadband Services funding category. In this category (and unchanged in the draft FY2016 version), the ESL states:

> Services provided by a third party for the operation, management, and monitoring of eligible broadband internal connections are eligible managed internal broadband services (e.g., managed Wi-Fi).

It is clear from the FY2015 (and draft FY2016) Eligible Services List that Managed Internal Broadband Services include not only the professional services required for the *operation* of an applicant’s local area network, but also the *management and monitoring* of the network as well. This treatment seems straightforward to us, and makes sense within the context of most managed LAN/Wi-Fi solutions.

Where we observe confusion among E-rate stakeholders, however, is how network management and monitoring solutions are treated in the other two areas of Category Two services: Internal Connections and Basic Maintenance. The Eligible Services List specifically identifies network management and monitoring functionality as *ineligible* as a Basic Maintenance service, and makes no statement on the purchase of management and monitoring hardware/software solutions in Internal Connections (although our presumption is that because the purchase of these components is not explicitly listed as eligible, it is assumed to be ineligible as described in the FY2015 *ESL Public Notice*.) So under Category Two, management and monitoring is addressed by the ESL in three ways:

- Not referenced in the Internal Connections section
- Referenced in the Managed Internal Broadband Services section as an eligible service
- Referenced in the Basic Maintenance section as an ineligible service

We question why this treatment is necessary under the new program rules which establish a per-student funding cap for Category Two funding requests and eliminate the program's "two-in-five" rule for Internal Connections requests. Further, how the ESL addresses management and monitoring functions leads to a number of odd questions, such as:

- If a network maintenance contract includes management and monitoring functionality, can the charges for those services be separated onto a Managed Internal Broadband Services funding request? What policy concern is served by this approach?
- As a practical matter, service providers who sell Managed Internal Broadband Services will use certain network management and monitoring hardware and software as a part of the provision of service to applicants. But it seems that those same hardware and software tools would not be eligible as Internal Connections components. Does this not show preferential treatment to managed service providers? If the overall functionality provided to the applicant is identical, why would management and monitoring provided as a service be eligible, but management and monitoring tools (for applicants to deploy and use on their own) be ineligible?

At a minimum, we would urge the Commission to clarify the eligibility of network management and monitoring hardware and software components in the Internal Connections funding category, as this seems to be a primary point of confusion and disagreement among stakeholders. In light of the introduction of Category Two budgets and the elimination of the two-in-five rule, and in the interest of simplicity and efficiency, we would like to see these functions administered consistently across all three Category Two funding categories. But at a minimum, we believe that explicitly clarifying the eligibility of these functions in each category would be very helpful.

THE ELIGIBLE SERVICES LIST'S DESCRIPTION OF "SOFTWARE" IS WIDELY MISINTERPRETED, AND SHOULD BE CLARIFIED

In a similar manner to firewalls, we find that there is a good deal of confusion among stakeholders regarding the eligibility of software. Primarily, we feel that this is a result of how the ESL is worded:

> Software supporting the components on this list used to distribute high-speed broadband throughout school buildings and libraries

It seems that the term "supporting" has a wide variety of interpretations, and we note that a number of service providers have claimed that various network functions should be eligible under this definition, including services like DNS, DHCP, directory services, mobile device management, and other functions. However, we do not feel that this was the Commission's intent, and the USAC eligibility decisions we have observed seem to indicate a pattern of approvals which are much more limited in scope.

Given this, we would suggest that the eligibility of software be clarified in the following manner:

> Eligible software includes:
>
> - Operating system software for the components on this list used to distribute high-speed broadband throughout school buildings and libraries
> - Virtual networking software which provides functionality equivalent to eligible broadband distribution hardware (such as Software Defined Networking components)

We feel that these clarifications would be of tremendous help to E-rate stakeholders, and could also increase the efficiency with which funding decisions could be made by the administrator by reducing potential "scope creep" for eligible services.

Respectfully submitted,

FUNDS FOR LEARNING, LLC

John D. Harrington
Chief Executive Officer
jharrington@fundsforlearning.com
405-341-4140

Funds For Learning, LLC
2575 Kelley Pointe Parkway Suite 200
Edmond, OK 73013

June 22, 2015